Office of the Governor
State Chief Information Officer

Security Policy

Title: Enterprise Authentication and Authorization Services Policy

Purpose: This policy establishes responsibility for establishment and maintenance of an authentication and authorization service. The authentication and authorization service provides a secure, consistent infrastructure for authenticating persons and controlling application access. This infrastructure is required for creating and maintaining an efficient, effective, statewide foundation that supports secure streamlined services.

Scope: This policy applies to all public agencies, their agents or designees subject to N.C.G.S. Article 3D of Chapter 147, "State Information Technology Services." Use by local governments, LEAs, community colleges, constituent institutions of the University of North Carolina and other public agencies is encouraged to the extent allowed by general statutes.

POLICY STATEMENT

An authentication and authorization service for controlling access to individual applications is an enterprise-wide infrastructure. It must be implemented and maintained by the Office of Information Technology Services as a statewide initiative in a directory based environment. Agencies that need centralized network infrastructure services, such as PKI, will be required to use this directory and adhere to the directory service standards.

An authentication and authorization service is founded in directory-based services and is a core technology for securing the state's infrastructure. Directory based services can provide strong and flexible authentication services for individuals and applications and must be consistent with the architecture and standards established by the State Chief Information Officer. Directory based authentication and authorization services must meet the following requirements:

- Security – Enterprise authentication and authorization services provide a secure environment for the creation and management of user identification (IDs). The Authentication and Authorization Services support authentication, minimize redundant application-based IDs, and integrate with the state's security infrastructure.

- Management – The authentication and authorization service and associated directory structure provides the state with consistent user accounts with minimal redundancy. The authentication and authorization service also provides users with the ability to maintain certain attributes of their account thereby reducing the workload of LAN administrators.

- Operation - An enterprise structure used for authentication and authorization, operated 24 hours a day and 7 days a week, is required to ensure that proper authentication and

authorization services are available. Unscheduled service interruptions interfere with conducting the state's electronic business securely as well as worker productivity.

- Scalability – An enterprise directory structure with authentication and authorization services are required to support long-term needs for statewide security of networks, applications and data. There should be no technical limitation that precludes servicing any audience permitted by general statute.

AUTHORITY

The State CIO is authorized to adopt this policy. G.S. §147-110.